WHAT IS CLAIMED IS:

1. A modular arithmetic apparatus for executing base conversion or base extension from a certain base as an input of a plurality of base elements to another base in a predetermined arithmetic algorithm in a residue number system, comprising:

a plurality of arithmetic units configured to input the base elements and execute calculation of the base conversion or base extension in units of the base elements by combining multiplication, addition, and modular arithmetic operation including the calculation of a specific term;

a k calculating unit configured to approximate an unknown parameter k for the base conversion or base extension to a carry generated by cumulative addition of a previous calculation result;

a switching section configured to switch enabling/disabling calculation of the specific term in the base conversion or base extension in accordance with the unknown parameter k output from said k calculating unit; and

a storing section configured to store the calculation result calculated by the arithmetic unit and provide the calculation result to said k calculating unit.

2. An apparatus according to claim 1, wherein said k calculating unit approximates a denominator in

an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem by a power of 2.

3. An apparatus according to claim 1, wherein

said apparatus further comprises bit selection unit, and

said $\underline{k}$ calculating unit approximates a numerator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem on the basis of round-down of a portion other than an effective bit length by said bit selection unit.

4. An apparatus according to claim 1, wherein said $\underline{k}$ calculating unit approximates a denominator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem by a power of 2 and approximates a numerator in the equation on the basis of round-down of a portion other than an effective bit length.

5. An apparatus according to claim 1, wherein the predetermined arithmetic algorithm comprises a Montgomery multiplication algorithm which outputs xyB^{-1} mod N or xyB^{-1} mod N + N for input integers $\underline{x}$, $\underline{y}$, and N.

6. An apparatus according to claim 5, wherein said arithmetic unit performs a power modular arithmetic operation in accordance with a predetermined algorithm using the Montgomery multiplication.

7. An apparatus according to claim 1, wherein said arithmetic unit performs a conversion configured

to convert residue number system representation into radix representation in accordance with a predetermined equation including an unknown parameter based on the Chinese remainder theorem.

8. A modular arithmetic apparatus for executing base conversion or base extension from a certain base as an input of a plurality of base elements to another base in a predetermined arithmetic algorithm in a residue number system, comprising:

a plurality of $\underline{k}$ calculating units configured to approximate an unknown parameter $\underline{k}$ for the base conversion or base extension to a carry generated by cumulative addition of a previous calculation result;

a plurality of switching sections, connected in series to one of said $\underline{k}$ calculating units, configured to switch for switching enabling/disabling calculation of a specific term in the base conversion or base extension in accordance with the unknown parameter $\underline{k}$ output from said one of $\underline{k}$ calculating units;

a plurality of arithmetic units connected in series to one of said switching sections to execute calculation of the base conversion or base extension in units of base elements by combining multiplication, addition, and modular arithmetic operation including the calculation of the specific term; and

a connection section provided for each of the arithmetic units for a connection to another set of

said $\underline{k}$ calculating unit, switching section, and arithmetic unit.

9. An apparatus according to claim 8, wherein said one of $\underline{k}$ calculating units approximates a denominator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem by a power of 2.

10. An apparatus according to claim 8, wherein said one of $\underline{k}$ calculating units approximates a numerator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem on the basis of round-down of a portion other than an effective bit length.

11. An apparatus according to claim 8, wherein said one of $\underline{k}$ calculating unit approximates a denominator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem by a power of 2 and approximates a numerator in the equation on the basis of round-down of a portion other than an effective bit length.

12. An apparatus according to claim 8, wherein the predetermined arithmetic algorithm comprises a Montgomery multiplication algorithm which outputs xyB^{-1} mod N or xyB^{-1} mod N + N for input integers $\underline{x}$, $\underline{y}$, and N.

13. An apparatus according to claim 12, wherein said arithmetic units perform a power modular arithmetic operation in accordance with a predetermined algorithm using the Montgomery multiplication.

14. An apparatus according to claim 8, wherein said arithmetic units perform a conversion configured to convert residue number system representation into radix representation in accordance with a predetermined equation including an unknown parameter based on the Chinese remainder theorem.

15. A modular arithmetic method of executing base conversion or base extension from a certain base as an input of a plurality of base elements to another base in a predetermined arithmetic algorithm in a residue number system, the method comprising:

executing calculation of the base conversion or base extension in units of base elements by combining multiplication, addition, and modular arithmetic operation including the calculation of a specific term;

approximating an unknown parameter $\underline{k}$ for the base conversion or base extension to a carry generated by cumulative addition of a previous calculation result;

switching enabling/disabling calculation of the specific term in the base conversion or base extension in accordance with the output unknown parameter $\underline{k}$; and

repeating the execution of the calculation of the base conversion or base extension.

16. A method according to claim 15, further comprising approximating a denominator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem by a power of 2.

17. A method according to claim 15, further comprising approximating a numerator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem on the basis of round-down of a portion other than an effective bit length.

18. A method according to claim 15, further comprising approximating a denominator in an equation of the unknown parameter $\underline{k}$ based on the Chinese remainder theorem by a power of 2 and approximating a numerator in the equation on the basis of round-down of a portion other than an effective bit length.

19. A method according to claim 15, wherein the predetermined arithmetic algorithm comprises a Montgomery multiplication algorithm which outputs xyB^{-1} mod N or xyB^{-1} mod N + N for input integers $\underline{x}$, $\underline{y}$, and N.

20. A modular arithmetic apparatus comprising:

a plurality of product-sum circuits configured to input a plurality of base elements and execute modular arithmetic operation; and

a correction term calculation unit configured to input the base elements and calculate a correction term to be used for said modular arithmetic operation in the product-sum circuits,

wherein

said correction term calculation unit sequentially calculates the correction term in units of bits, and

each of said product-sum circuits sequentially

reflects the correction term calculated by said correction term calculation unit and performs base conversion or base extension.

21. An apparatus according to claim 20, wherein said product-sum circuit performs a Montgomery multiplication.

22. An apparatus according to claim 20, wherein said correction term calculation unit sequentially calculates the correction term in units of bits, and each of said product-sum circuits sequentially reflects the correction term calculated by said correction term calculation unit and converts a residue number system representation into a radix representation.

23. An apparatus according to claim 20, wherein said correction term calculation unit comprises a division circuit, and

a base of a residue number system processed by said product-sum circuit is approximated to a power of 2.

24. An apparatus according to claim 20, further comprising a bit selection section configured to select an upper bit of the input to said correction term calculation unit.

25. An apparatus according to claim 20, further comprise an I/O section for inputting/outputting data to/from an external unit.